Digitization of enterprises is no longer restricted to the ERP or CRM systems. Higher education institutions, around the globe, are taking the steps towards a digital transformation. modern-day organizations are traveling on a fast-moving digital highway and are using a wide range of applications, primarily cloud based. However, leveraging cloud does not take away the security risks.

Are Passwords Really Outdated?

Usernames and passwords were invented back in 1964. Despite attempts to make static credentials more secure by adopting 2FA (two-factor authentication), utilizing OTPs, SMSs, or hardware tokens, organizations are still vulnerable to phishing attacks, keylogging and other forms of cyberattacks.

According to the 2019 Verizon Breach Investigations Report, compromised credentials are the reason behind 80% of all data breaches in 2019. Corporations and institutions of higher education are aware of the security risks associated with shared or stolen passwords and they are looking for solutions to help secure their applications. The perpetual onslaught of breaches over the last decade has clearly shown that passwords have become more vulnerable than ever.

Millions of dollars are spent on authentication, but still, users across different organizations and institutions use passwords to login to their systems/applications. This is because traditional MFA products still rely on passwords, leaving an opportunity for hackers to steal those credentials. Therefore, it has become important for organizations to deploy a powerful login strategy than can fortify security.

The New Era of Authentication is PASSWORDLESS

By eliminating the past reliance on security credentials (usernames and passwords), passwordless authentication strengthens organizational security by removing the risk of compromised credentials. Going Passwordless means being able to verify a user's identity without passwords. This is now the future of cybersecurity.

Gartner predicts, 60% of large and global enterprises and 90% of mid-sized enterprises will implement passwordless workflows in more than half of their required use cases.

The Problem with Passwords

Relying on passwords for security was developed with good intent but eliminating passwords altogether with passwordless authentication can be a far better option. A password and a second-factor policy still retain the inherent flaws of passwords, plus users still have to remember passwords and safeguard secrets, so the security risk of password reuse continues to exist. Here are a few issues associated with passwords:

1. Passwords negatively impacts the User Experience

An average internet user has around 118 online accounts that require a password, and this number is expected to reach around 300 by 2022. It is a big challenge to keep track of so many credentials for an average user. Further, password complexity requirement vary application to application.

The probability of remembering passwords to all these accounts is extremely difficult unless the user has same password for all applications. This hinders the user experience and drastically reduces productivity.

2. Passwords are threats to Security Environments

Passwords are the common avenue for identity attacks. There have been a number of breaches in the past due to weak or stolen passwords. Account takeover attacks and brute force attacks can actually deteriorate the security infrastructure of an organization.

Also, threats like man-in-the-browser attacks and man-in-the-middle attacks aim to take advantage by mimicking a login screen while encouraging the user to enter passwords. By requiring passwords, service providers are inadvertently putting users at risk to these types of threats.

3. Passwords are costly for IT

Beyond the security headaches that password resets create, passwords are expensive to manage for an IT organization. The lost and forgotten passwords need to be reset, most of the time through the help desk, which introduces downtime and expense.

Large organizations spend up to $1 million every year on staffing and infrastructure simply to reset passwords- what a productivity loss for the IT help desk personnel but also for the end users waiting to get assistance.

How does Passwordless authentication works?

Passwordless authentication is a type of multi-factor authentication (MFA), but one which replaces passwords with more secure authentication factors such as TouchID, FaceID or PIN. Authentication without passwords relies on the same principles as digital certificates – having a cryptographic key pair with a public and private key. Think of a public key as a padlock and private key as a real key that unlocks that padlock. The public key is provided to the browser, application, website or other online system(s) for which a user wants to access while the private key is stored in user's local device and is tied to an authentication factor such as PIN, FaceID or fingerprint.

Why Passwordless Authentication? – The Untold Benefits

Authentication without passwords gives organizations a massive leap forward in terms of their security posture.

- **Enhanced User Experience**: When users do not have to memorize and safeguard their passwords the authentication process gets more streamlined.

- **Improved Security**: Passwords have been vulnerable since the time they were discovered. Passwords are the biggest attack vector that are at risk to account takeover attacks, credential stuffing, brute force attacks, password spraying and more. No passwords mean better security.

- **Reduction in Operation Costs**: Passwords are expensive to maintain and require constant maintenance from IT staff and need to be changed on a regular basis. According to research, approximately 50% of help desk calls are related to password resets, sometimes even higher. According to Forrester, the cost of a single password reset can be as high as $70. With Passwordless Authentication, there are no passwords and the cost for resetting lost/forgotten passwords can be greatly reduced and/or even eliminated.

- **Better Control and Visibility to IT**: Sharing and reuse of passwords are common issues with password-based authentication. With the introduction of passwordless authentication in an organization's security infrastructure, IT can reclaim its purpose of having complete visibility over identity and access management.

- **Scalability**: Passwordless authentication is totally scalable as end users already possess authentication factors such as their mobile device (authenticator apps, biometrics, SMS etc.) or laptop (Touch ID, FaceID, Email etc.)

The Future without Passwords

A comprehensive passwordless authentication solution for customers, partners and employees across all channels and devices will make an organization more secure. Going Passwordless reinvents the authentication wheel providing a better user experience, strengthens organizational security, and gives better overall control to IT. Corporations have already started deploying various forms of passwordless authentication, the world is going passwordless.

Go PASSWORDLESS with QuickLaunch's **Passwordless Authentication**.